TrickBot Malware Research

Michael Twining

Department of Criminal Justice Studies, Utica University

[REDACTED]

[REDACTED]

[REDACTED]

TrickBot Malware Research

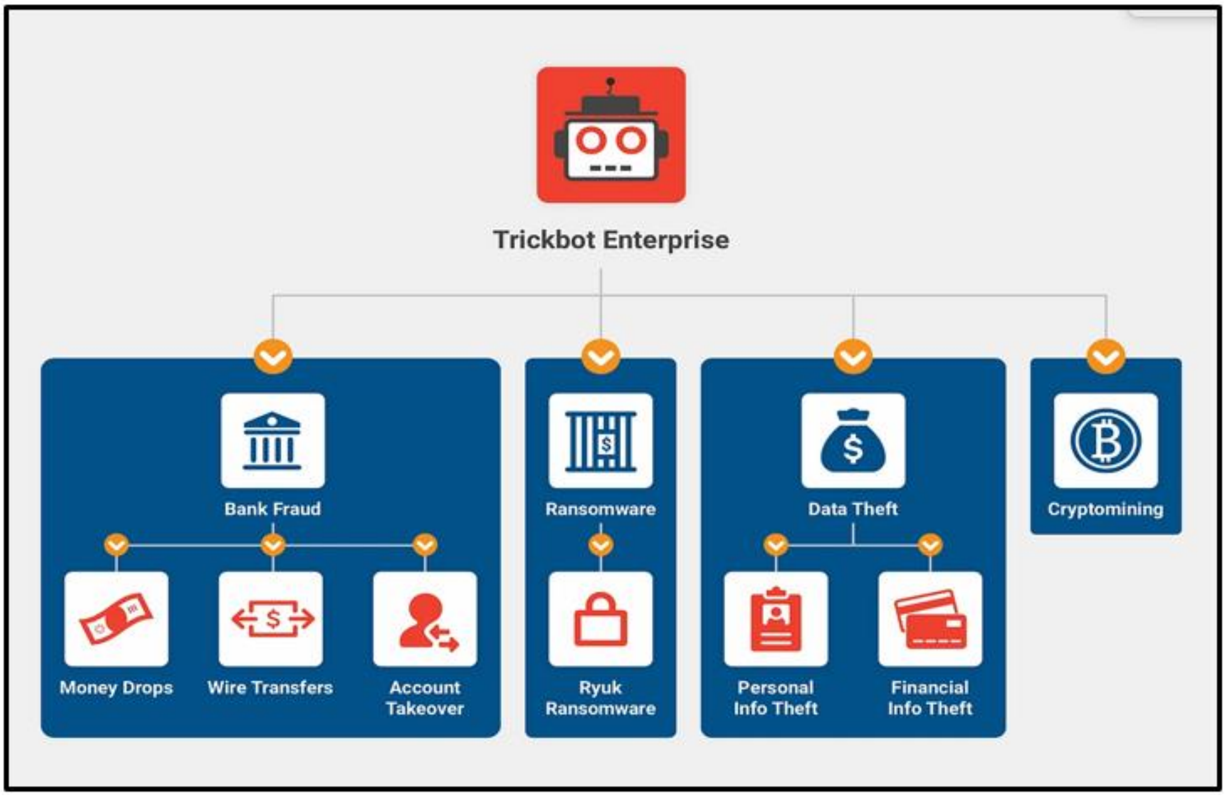
There are many threats to endpoint and network infrastructure, with malicious intent for financial gain as a motive. Threat actors can come from all over the world. One example of this TrickBot operators. Thought to be from Russia, other aliases of this group are known as Wizard Spider, UNC1878, and Gold Blackburn (CISA, 2021). TrickBot malware is unique in that it has the capabilities to work in tandem with other ransomware and malware. Because of this, it is becoming more common to see the collaboration between cyber-criminals attacking high-valued targets (CISA, 2021). TrickBot was first discovered in 2016 as a banking trojan, but a descendant of ZeuS banking trojan from 2005 and Dyre which shut down in 2015. In fact, some of TrickBot's capabilities come from Dyre's original code (MS-ISAC, 2021). Banking trojans are malware that are intended to gain access onto a victim's machine through the installation of the program, either from clicking on a compromised URL or an attachment on an email, for stealing credentials. Over time, it developed with other capabilities, making it more dangerous to defenders, as it constantly evolves and changes signatures that are used to defend against their attacks. One of these capabilities is the ability to self-propagate on a network through server message block (SMB) protocol (Cybersecurity and Infrastructure Security Agency, 2021). This is a common feature with a worm. What makes this even more dangerous is that other malicious programs are loaded after deployment of TrickBot. Once it has propagated all over a network without being caught and then deploys ransomware, then it has the ability shut down all operations of the target. An example of this was seen in 2019, where the relationship between Ryuk Ransomware and TrickBot became more apparent (MS-ISAC, 2021). In Fall of 2020, it was reported that the US Cyber Command and private sector thwarted TrickBot attacks with intent to interfere with the election process (MS-ISAC, 2021).

TrickBot has many uses including bank fraud, data theft, crypto mining, and deploying ransomware (MS-ISAC, 2021). Figure 1 illustrated the specific outcomes from these uses, including taking over bank accounts, exfiltrating personal information, and performing wire transfers and money drops (MS-ISAC). SMB is a protocol used for sharing files, printers, and other network resources. Given the capabilities of exploiting SMB to propagate on a network, these other uses can exponentially increase in their impact to individuals and organizations. Because SMB is native to Windows machines, proper configuration is needed to avoid exploitation of default settings. With the loading of ransomware capabilities, this can cripple an organization quickly.

While it has a robust command-and-control infrastructure, that also means that there should be indicators in network traffic. This could be through common or uncommon ports through the internet to unknown IP addresses and domains. Detection is key to mitigating the impacts, as once TrickBot has gained a foothold in a network, it is costly and time-consuming to remove all of the malware. Once detected, containment is important to prevent the spread. Again, if ransomware is deployed, limiting the exposure of the network impacted can help reduce the impact of the ransomware event. TrickBot has been known to deploy Emotet, Conti, and Ryuk Ransomware by implementing logic to deploy later to avoid detection from a security event (Cybersecurity and Infrastructure Security Agency, 2021). This delayed deployment strategy allows TrickBot to remain hidden, increasing the risk that even after an organization has recovered from a ransomware event, TrickBot may still reside on backups, posing a continued threat.

Figure 1

Overview of TrickBot's enterprise model. Source: Bleeping Computer (MS-ISAC, 2021)



The tactics and techniques used by TrickBot are many, but similar like many malware it begins with initial access by spear phishing with a malicious attachment or link (Cybersecurity and Infrastructure Security Agency, 2021). For execution, The malware creates scheduled tasks on the system to maintain persistence, runs macros from attachments to download and deploy on the victim’s machine, installs a java script file that when opened communicated to the C2 servers (if malicious link clicked instead) which downloads the malware, and then uses Windows API to create processes and manage execution flow (Cybersecurity and Infrastructure Security Agency, 2021). Another persistence tactic is that it creates an autostart service, so it starts as the machine boots (Cybersecurity and Infrastructure Security Agency, 2021). It does have some forms of defense evasion tactics, including modifying registry entries, process hollowing, comes with signed downloader component so it appears trusted, disables Windows Defender, and is packed, so it’s initial code is not seen by the system or defender as malicious (Cybersecurity and Infrastructure Security Agency, 2021). TrickBot will enumerate the victim’s machine and network details, as well as enumerate files and passwords and sends the information over though the C2 server (Cybersecurity and Infrastructure Security Agency, 2021). It has been known to encrypt this traffic over HTTP (Cybersecurity and Infrastructure Security Agency, 2021).

TrickBot has a history where the constant has been change. The ability to self-propagate on a network, and then later deploy ransomware makes it extremely dangerous. The designers of the malware implement techniques that help evade detection, like changing the IP addresses that the C2 servers use and changing them frequently. What is most impressive is the modular nature of the malware, making it enticing for other cybergangs to use to deploy their own malware. Imagine if you will, the ability to not only attack a large company once successfully but attack it multiple times. That is what TrickBot’s evasion tactics potentially enable. However, like other malware that connects to a C2 server, communication is where it could be identified to the defender who is looking for it, such as encrypted traffic through HTTP to an unknown resolved domain name or IP address. One of the best defenses against it is train to employees on how to spot a phishing email, and to how to report them so that defenders can mitigate the risk of attack. Also ensure that defaults for using SMB, if necessary, are configured properly and if not needed, disable. Lastly, because of the changing nature of the malware, defenders should stay on top of trends and new malware samples to harden systems from future attacks.

References

CISA. (2021, March). Fact sheet: TrickBot malware. https://www.cisa.gov/sites/default/files/publications/TrickBot_Fact_Sheet_508.pdf.

Cybersecurity and Infrastructure Security Agency. (2021, May 20). *TrickBot malware*. Cybersecurity Advisory. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a.

MS-ISAC. (2021, April 22). *Blog: TrickBot: Not your average hat trick - a malware with multiple hats*. CIS. https://www.cisecurity.org/insights/blog/trickbot-not-your-average-hat-trick-a-malware-with-multiple-hats.